ELECTRONIC CONFERENCE SYSTEM, ELECTRONIC CONFERENCE METHOD, PROGRAM, AND STORAGE MEDIUM

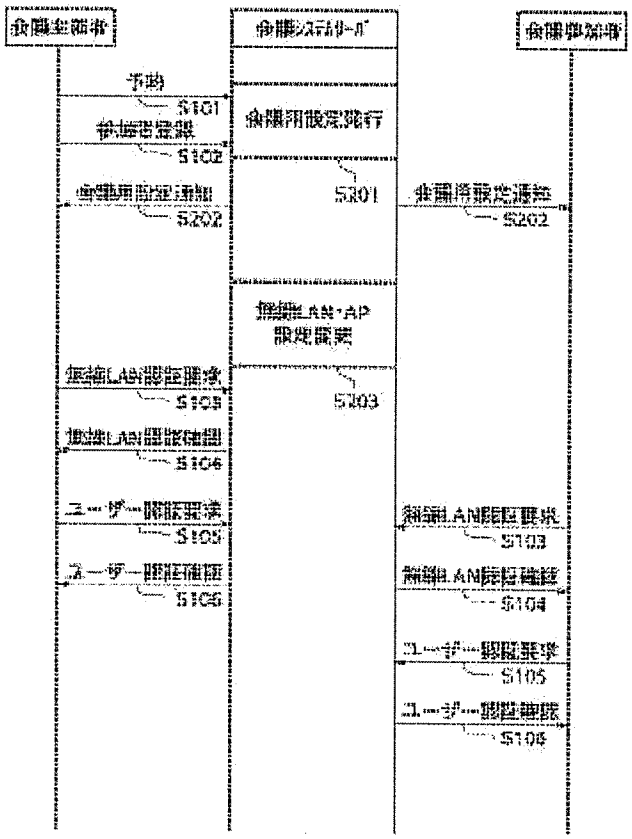
Publication number: JP2003304518 (A)
Publication date: 2003-10-24

Inventor(s): NAGO HIDETADA +
Applicant(s): CANON KK +

Classification:
- international: ***H04N7/15; H04L12/28; H04M3/56;*** **H04N7/15; H04L12/28; H04M3/56;** (IPC1-7): H04N7/15; H04L12/28; H04M3/56
- European:
Application number: JP20020109364 20020411
Priority number(s): JP20020109364 20020411

Abstract of **JP 2003304518 (A)**

PROBLEM TO BE SOLVED: To provide an electronic conference system in which participants can take participation without the need for a special work and which can prevent a malicious act by a third party such as interception of contents of the conference. ; SOLUTION: A conference sponsor makes a reservation for a conference at a conference system server 2 (S101) and registers electronic mail addresses of conference participants (S102). The conference system server 2 issues conference purpose setting information such as accounts and passwords different from the participants (S201), and transmits electronic mail describing the contents of the information to the conference sponsor and the conference participants (S202). Each participant starts a conference system installed on its own terminal 4 and allows the conference system to read the conference purpose setting information described in the notified electronic mail to take participation in the conference. ; COPYRIGHT: (C)2004,JPO



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－304518
（P2003－304518A）
(43)公開日　平成15年10月24日(2003.10.24)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　7/15	６５０	Ｈ０４Ｎ　7/15	６５０	５Ｃ０６４
Ｈ０４Ｌ　12/28	３００	Ｈ０４Ｌ　12/28	３００Ｚ	５Ｋ０１５
Ｈ０４Ｍ　3/56		Ｈ０４Ｍ　3/56	Ｃ	５Ｋ０３３

審査請求　未請求　請求項の数12　ＯＬ　（全 13 頁）

(21)出願番号　特願2002－109364(P2002－109364)

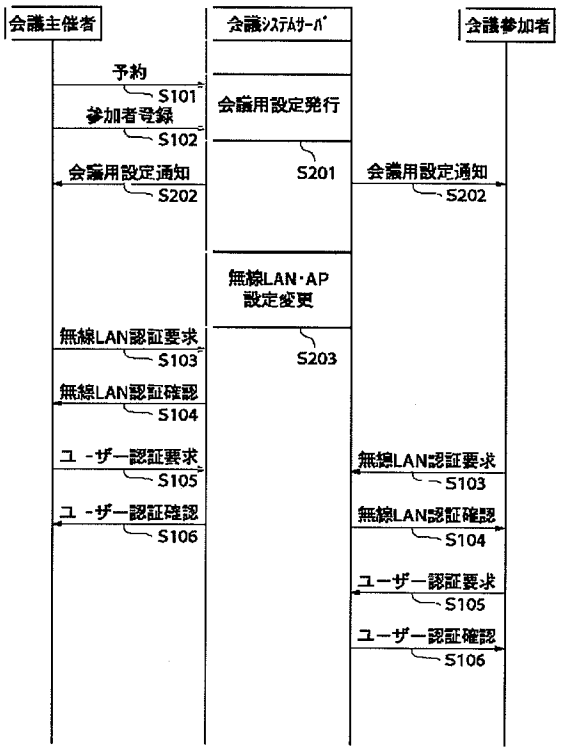
(22)出願日　平成14年４月11日(2002.4.11)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　名合　秀忠
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100081880
弁理士　渡部　敏彦

Ｆターム(参考)　5C064 AA02 AC02 AC06 AC12 AC16 AC18 AC22
5K015 AA10 AB01 AF06 JA02
5K033 AA08 DA17

(54)【発明の名称】　電子会議システム、電子会議方法、プログラムおよび記憶媒体

(57)【要約】
【課題】　参加者が特別な作業を行うことなく会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる電子会議システムを提供する。
【解決手段】　会議主催者は、会議システムサーバ２に会議の予約を行い（Ｓ１０１）、会議参加者の電子メールアドレスを登録する（Ｓ１０２）。会議システムサーバ２は参加者毎に異なるアカウントおよびパスワード等の会議用設定情報を発行し（Ｓ２０１）、その内容を記載した電子メールを送る（Ｓ２０２）。参加者は、所有する端末４に搭載されている会議システムを起動させ、通知された電子メールに記載されている会議設定情報を読み込ませることで、会議に参加する。



【特許請求の範囲】

【請求項１】　ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議システムにおいて、

会議の予約を行い、この会議への参加者を登録する登録手段と、

前記登録された参加者にそれぞれ固有の識別情報を発行する発行手段と、

前記発行した識別情報を前記登録された参加者が所有する端末に通知する通知手段と、

前記ネットワークに接続された端末が前記クライアントして起動した場合、前記通知された識別情報を取得する取得手段と、

前記クライアントの識別情報の認証を前記会議サーバに要求する要求手段と、

前記認証を要求された識別情報が有効であるか否かを判断する判断手段と、

前記識別情報が有効である場合、前記クライアントに会議への参加を許可する許可手段とを備えたことを特徴とする電子会議システム。

【請求項２】　前記会議サーバと有線ネットワークを介して通信可能であり、前記クライアントと無線ネットワークを介して通信可能である無線通信装置を備え、

前記通知手段は、前記識別情報とともに、前記無線通信装置と無線通信を行うための通信設定情報を通知し、

前記端末は、前記通知された通信設定情報を基に、前記無線通信装置と無線通信を行うための設定を変更することを特徴とする請求項１記載の電子会議システム。

【請求項３】　前記会議サーバは、前記クライアントと無線ネットワークを介して無線通信を行う無線通信手段、前記登録手段、前記発行手段および前記通知手段を備え、前記無線通信を行うための通信設定情報を決定し、前記識別情報とともに、前記決定された通信設定情報を通知し、

前記クライアントは、前記取得手段を備え、前記会議サーバから通知された通信設定情報を前記識別情報と共に取得し、該取得した通信設定情報を基に、前記会議サーバとの無線通信を確立することを特徴とする請求項１記載の電子会議システム。

【請求項４】　前記会議サーバとは別のネットワーク上に設けられた予約サーバは、前記登録手段、前記発行手段および前記通知手段を備え、前記会議サーバと無線通信を行うための通信設定情報を決定し、該決定した通信設定情報および前記識別情報を通知するとともに、前記通信設定情報を着脱式の記録媒体に記憶しておき、

前記会議サーバは、前記クライアントと無線ネットワークを介して無線通信を行う無線通信手段を備え、前記記録媒体に記憶された通信設定情報を基に、前記無線通信を行うための設定を変更し、

前記クライアントは、前記取得手段を備え、前記予約サーバから通知された通信設定情報を前記識別情報と共に取得し、該取得した通信設定情報を基に、前記会議サーバとの無線通信を確立することを特徴とする請求項１記載の電子会議システム。

【請求項５】　前記会議サーバは、前記クライアントと無線ネットワークを介して無線通信を行う無線通信手段、前記登録手段、前記発行手段および前記通知手段を備え、前記無線ネットワークとは別のネットワークに接続・切り離し自在であり、該別のネットワークに接続された状態で、前記会議の予約を行い、この会議への参加者を登録し、該会議サーバと無線通信を行うための通信設定情報を決定し、該決定した通信設定情報および前記識別情報を通知するとともに、前記無線通信を行うための設定を変更し、

前記クライアントは、前記取得手段を備え、前記会議サーバから通知された通信設定情報を前記識別情報と共に取得し、該取得した通信設定情報を基に、前記会議サーバとの無線通信を確立することを特徴とする請求項１記載の電子会議システム。

【請求項６】　前記登録手段は、前記参加者の電子メールアドレスを登録し、前記通知手段は前記登録された電子メールアドレス宛に電子メールで通知することを特徴とする請求項１乃至５のいずれかに記載の電子会議システム。

【請求項７】　全ての参加者のログアウト処理が行われると、会議終了とみなし、所定時間内に次の会議の予定がある場合、前記無線通信装置の設定を次の会議用のものに変更する一方、前記所定時間内に次の会議の予定がない場合、ランダムに生成された通信設定情報を基に、前記無線通信装置の設定を変更することを特徴とする請求項２記載の電子会議システム。

【請求項８】　全ての参加者のログアウト処理が行われると、会議の終了とみなし、前記無線通信手段の電源をオフにするか、あるいは前記会議サーバの全電源をオフにすることを特徴とする請求項３乃至５のいずれかに記載の電子会議システム。

【請求項９】　前記会議サーバは、前記判断手段を備え、前記認証を要求された識別情報と同一の識別情報を有する参加者が既に存在する場合、その旨の警告を参加者に送信することを特徴とする請求項１乃至８のいずれかに記載の電子会議システム。

【請求項１０】　ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議方法において、

会議の予約を行い、この会議への参加者を登録するステップと、

前記登録された参加者にそれぞれ固有の識別情報を発行するステップと、

前記発行した識別情報を前記登録された参加者が所有する端末に通知するステップと、

前記ネットワークに接続された端末が前記クライアントして起動した場合、前記通知された識別情報を取得するステップと、
前記クライアントの識別情報の認証を前記会議サーバに要求するステップと、
前記認証を要求された識別情報が有効であるか否かを判断するステップと、
前記識別情報が有効である場合、前記クライアントに会議への参加を許可するステップとを有することを特徴とする電子会議方法。
【請求項１１】　請求項１０に記載の電子会議方法を実現するためのコンピュータ読み取り可能なプログラムコードを保持する記憶媒体。
【請求項１２】　請求項１０に記載の電子会議方法を実現するためのコンピュータ読み取り可能なプログラムコードを有するプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、会議室において、電子データを共有して会議を行う電子会議システム、電子会議方法、プログラムおよび記憶媒体に関する。
【０００２】
【従来の技術】従来、会議は、一般的に資料となる書類を配布して進められる。しかし、近年、書類の代わりに、電子データをやり取りし、資料を電子的に改変しながら進める電子会議システムが知られている。例えば、特開平０９－０８１４８９号公報に示される有線ネットワークによる電子会議システムでは、会議に参加できない場合でも、その参加できない人の資料だけは会議で使えるようにすることが提案されている。
【０００３】
【発明が解決しようとする課題】しかしながら、従来の電子会議システムでは、以下に掲げる問題があり、その改善が要望されていた。コンピュータ等の端末を会議室に持ち込み、その端末を有線ＬＡＮに接続して会議を行う場合、ＩＰアドレスなどのネットワークの設定を変更する必要があったり、ＬＡＮケーブルを会議室内に引き回すといった煩わしさがあった。
【０００４】こういう煩わしさを解消するために、会議用サーバと、会議に参加する人の端末との間で無線通信を採用する方式が提案されている。一般的には、ＩＥＥＥ８０２．１１で規定された無線ＬＡＮが用いられている。
【０００５】しかし、無線は広がりを持ったある範囲に伝幡するので、特定の相手のみに送ることができず、悪意のある第三者の盗聴を受けるおそれがあった。また、悪意のある第三者に無線の設定が知られると、ネットワークに侵入されるという無線特有の問題が生じるおそれがあった。
【０００６】上記特開平０９－０８１４８９号公報の電子会議システムでは、有線ネットワークを前提としており、無線化によるセキュリティの脆弱性は考慮されていなかった。また、グループ全員が同一内容のグループリストを有し、グループリストを基に暗号化鍵を生成する方法が提案されている。会議のように、メンバーが会議毎に入れ替わるような場合、あまり使い易い方法とはいえなかった。
【０００７】また、特開平０５－４８７４６号公報の電子会議システムでは、会議毎にコード番号を発行し、会議参加時にコード番号を入力するといった方法が提案されている。しかし、無線化した場合、覚え易い短めのコードだと容易に第三者に知られ、会議内容のセキュリティを確保することが難しかった。さらに、有線と同様、ネットワークの設定など、各種の設定が必要であった。
【０００８】そこで、本発明は、参加者が特別な作業を行うことなく会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる電子会議システム、電子会議方法、プログラムおよび記憶媒体を提供することを目的とする。
【０００９】
【課題を解決するための手段】上記目的を達成するために、本発明の電子会議システムは、ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議システムにおいて、会議の予約を行い、この会議への参加者を登録する登録手段と、前記登録された参加者にそれぞれ固有の識別情報を発行する発行手段と、前記発行した識別情報を前記登録された参加者が所有する端末に通知する通知手段と、前記ネットワークに接続された端末が前記クライアントして起動した場合、前記通知された識別情報を取得する取得手段と、前記クライアントの識別情報の認証を前記会議サーバに要求する要求手段と、前記認証を要求された識別情報が有効であるか否かを判断する判断手段と、前記識別情報が有効である場合、前記クライアントに会議への参加を許可する許可手段とを備えたことを特徴とする。
【００１０】本発明の電子会議方法は、ネットワークを介して会議サーバおよびクライアントが接続され、電子データを共有することで会議を行う電子会議方法において、会議の予約を行い、この会議への参加者を登録するステップと、前記登録された参加者にそれぞれ固有の識別情報を発行するステップと、前記発行した識別情報を前記登録された参加者が所有する端末に通知するステップと、前記ネットワークに接続された端末が前記クライアントして起動した場合、前記通知された識別情報を取得するステップと、前記クライアントの識別情報の認証を前記会議サーバに要求するステップと、前記認証を要求された識別情報が有効であるか否かを判断するステップと、前記識別情報が有効である場合、前記クライアントに会議への参加を許可するステップとを有することを

特徴とする。

【００１１】

【発明の実施の形態】本発明の電子会議システム、電子会議方法、プログラムおよび記憶媒体の実施の形態について、図面を参照しながら説明する。

【００１２】［第１の実施形態］図１は第１の実施形態における電子会議システムの構成を示す図である。図において、１は無線ＬＡＮアクセスポイントである。２は会議システムサーバである。３は有線ＬＡＮである。４は会議で使用する端末である。

【００１３】図２は会議の予約から会議開始時までの動作処理手順を示すフローチャートである。本実施形態では、無線通信方式にＩＥＥＥ８０２．１１で規定されている無線ＬＡＮを用いる場合を示す。

【００１４】会議室には、通常の無線ＬＡＮアクセスポイント（ＡＰ）１が存在し、会議システムを運営するサーバ２は別の場所に存在する。ここでは、このサーバ２を会議システムサーバ２と称する。ＡＰ１および会議システムサーバ２は、有線ＬＡＮ３で接続されている。

【００１５】会議システムサーバ２は会議予約機能を有し、会議の主催者は、会議システムサーバ２上で会議を予約する（Ｓ１０１）。この予約の際、会議の日時、会議室、参加者のメールアドレスを登録する（Ｓ１０２）。

【００１６】会議システムサーバ２は、会議の予約を受け付けると、会議に必要な無線ＬＡＮの無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、さらに、予約された会議だけで有効なアカウントおよびパスワードを参加者分だけ発行する（２０１）。そして、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者にその電子メールを送る（Ｓ２０２）。

【００１７】このように、会議参加者宛ての電子メールには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードが記載されている。電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム（ソフトウェア）同士でのみ有効な符号に置き換えておくことが望ましい。会議システムサーバ２は、会議予約情報に、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、全ての参加者のアカウントおよびアカウントに対応するパスワードを記録する。

【００１８】各会議参加者は、会議システムサーバ２から送られてきた電子メールを会議で使用する端末４に渡し、端末４内の会議システム（ソフトウェア）を起動させて、会議システムサーバ２から送られてきた電子メールを読み込ませる。会議システムは、読み込んだ電子メールから会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを取り出して記憶する。

【００１９】複数の会議を管理するために、図３に示すような会議スケジュール管理を行う。図３は会議スケジュール管理を示す図である。会議参加者は、会議の日時と場所の情報だけを知り、会議の無線通信の設定情報やアカウントおよびパスワードについては、会議システムが管理するので、知らなくてよい。また、第三者の目に触れないためにも、会議参加者の目に触れさせない方が望ましい。

【００２０】会議を予約した時間になると、会議システムサーバ２は、会議で使用する無線ＬＡＮアクセスポイント１内の無線グループＩＤおよび無線ＬＡＮ用暗号化キーの設定を変更する（Ｓ２０３）。

【００２１】参加者は、会議システム（ソフトウェア）が搭載されている端末４を会議室に持ち込み、端末４を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループＩＤおよび無線ＬＡＮ用暗号化キーを端末４に接続されている無線ＬＡＮカードに設定する。端末４が無線ＬＡＮを内蔵している場合、内蔵無線ＬＡＮに設定する。

【００２２】会議システムは、無線ＬＡＮの接続要求（無線ＬＡＮ認証要求、Ｓ１０３）および接続完了後（無線ＬＡＮ認証確認、Ｓ１０４）、無線ＬＡＮを経由して同じ電子メールに記載されていたアカウントで会議システムサーバ２にログインし（ユーザ認証要求、Ｓ１０５）、パスワードで認証する（ユーザ認証確認、Ｓ１０６）。

【００２３】会議システムサーバ２は、アカウント名およびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。ここで、会議に代理人を出席させる場合、会議システムサーバ２から送られてきた電子メールを、転送するかあるいは記録媒体に記録して代理人に渡す。そして、代理人は会議に持ち込む端末４に搭載されている会議システムを起動させ、会議システムサーバ２から送られてきた電子メールを読み込ませる。出席者が変わっても、会議用のアカウントのみで有効な出席者であるか否かを判断するので、容易に代理人を出席させることが可能となる。

【００２４】同一のアカウントのログインが発生した場合、一方が不正なログインをしているおそれがある。これを検出するために、会議システムサーバ２は、会議が始まると、アカウントのログイン処理を行う。図４はアカウントのログイン処理手順を示すフローチャートである。この処理プログラムは、会議システムサーバ２内の記憶媒体に格納されており、会議システムサーバ２内のＣＰＵによって実行される。

【００２５】まず、ログイン要求があるまで待ち（ステップＳ１）、ログイン要求があると、同一ログインフラグを調べる（ステップＳ２）。同一ログインフラグが立

っていない（セットされていない）場合、今回ログイン要求されたアカウントと同じアカウントからのログイン要求が既にあったか否かを調べる（ステップＳ３）。同じアカウントからのログイン要求がなかった場合、正常なログイン処理を行い（ステップＳ４）、ステップＳ１の処理に戻り、次のログイン要求を待つ。

【００２６】一方、ステップＳ３で同一のアカウントからのログイン要求が既にあった場合、同一のアカウントからのログイン要求があったことを示す同一ログインフラグをセットし（ステップＳ５）、既にログインしている会議出席者の有無を調べる（ステップＳ６）。会議出席者がいない場合、ステップＳ１の処理に戻って、次のログイン要求を待つ。一方、既に会議出席者がいる場合、正常にログインした出席者に不正なログインがあった旨の警告を送信する（ステップＳ７）。この後、ステップＳ１の処理に戻る。

【００２７】そして、ステップＳ５で同一ログインフラグがセットされると、次にログイン要求があった場合、ステップＳ２における同一ログインフラグのチェックの結果、この会議には不正なログイン処理が行われている旨の警告を表示し（ステップＳ８）、ステップＳ１の処理に戻る。

【００２８】そして、不正なログインがあると、会議システムサーバ２は、会議主催者だけにアクセスを許可する。不正なログインの警告を目にした会議主催者は、会議システムサーバ２に会議用設定情報の再発行を依頼する。依頼を受けた会議システムサーバ２は、会議用設定情報を新たに決定し、その設定ファイルを会議主催者に渡す。渡された設定ファイルには、新しい無線グループＩＤ、無線ＬＡＮ用暗号化キー、この会議に共通のアカウントおよびパスワードが記載されている。主催者は、記録媒体を使用するか、あるいは無線ＬＡＮの１対１通信モードを使用して、他の参加者に新しい会議用設定情報を通知する。不正ログインを行った第三者が、この時点で新たな会議用設定情報を知ることは不可能であるので、会議内容を知ることはできない。会議システムサーバ２は、念のため、参加者のログイン数を調べ、予約時に登録されているメールアドレスの数とこのログイン数の比較を行う。

【００２９】尚、電子メールそのものに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードからなる会議用設定情報を記載する代わりに、電子メールにファイルを添付してもよく、この添付ファイルに会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載しておくことでも、同様の動作が実現可能である。

【００３０】また、全ての出席者のログアウト処理が行われると、会議システムサーバ２は、会議終了であると判断し、会議終了であると判断した会議用のアカウントおよびパスワードを破棄する。また、無線ＬＡＮアクセスポイント１の設定を次の会議用のものに変更する。ここで、次の会議の予定がない場合、あるいは次の会議まで長時間ある場合、ランダムに生成した無線グループＩＤおよび無線ＬＡＮ用暗号化キーでその設定を変更し、悪意の第三者の不正アクセスを防止する。

【００３１】このように、本実施形態では、会議予約時に発行する電子メールに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載し、参加者の端末に搭載されている会議システムに読み込ませるだけで、自動的に会議に参加でき、しかも第三者による会議内容の盗聴といった悪意ある行為を防止することができる。

【００３２】［第２の実施形態］図５は第２の実施形態における電子会議システムの構成を示す図である。前記第１の実施形態と同様の構成要素については、同一の符号を付すことにする。図において、３は有線ＬＡＮである。４は会議で使用する端末である。５は多機能アクセスポイントである。

【００３３】図６は多機能アクセスポイントの内部構成を示すブロック図である。図において、５１は制御部である。５２は無線ＬＡＮアクセスポイント部である。５３は不揮発性記憶部である。５４は着脱式記憶部である。５５は有線ＬＡＮインターフェイスである。無線ＬＡＮアクセスポイント部５２は、大人数で会議を行う際、トラフィックの分散を図るため、複数存在することもある。

【００３４】また、会議の予約から会議開始時の処理、および同一のアカウントのログインがあった場合の処理は、前記第１の実施形態における図２および図４と同様である。

【００３５】多機能無線ＬＡＮアクセスポイント（ＭＦＡＰ）５は会議室に設けられており、有線ＬＡＮ３に接続され、有線ＬＡＮ３側から会議の予約などが行うことが可能である。ＭＦＡＰ５では、会議の予約機能を有した会議システム（ソフトウェア）が動作しており、ＭＦＡＰ５は無線ＬＡＮアクセスポイントとしての機能の他、無線ＬＡＮ側と有線ＬＡＮ３側へのアクセスを可能にする機能を有する。したがって、図２における会議システムサーバの機能はＭＦＡＰ５によって実現されている。

【００３６】会議主催者は、希望する会議室に設置されているＭＦＡＰ５で会議の予約を行う（Ｓ１０１）。予約の際、会議の日時、参加者のメールアドレスを登録する（Ｓ１０２）。会議の予約を受け付けると、ＭＦＡＰ５は、会議に必要な無線ＬＡＮの無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、さらに、予約された会議だけで有効なアカウントおよびパスワードを参加

者分だけ発行する（Ｓ２０１）。

【００３７】登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（Ｓ２０２）。参加者宛ての電子メールには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードが記載されている。電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム（ソフトウェア）同士でのみ有効な符号に置き換えておくことが望ましい。ＭＦＡＰ５は、会議予約の情報に、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、全ての参加者のアカウントおよびこれらのアカウントに対応するパスワードを不揮発性記憶部５３に記憶する。

【００３８】ＭＦＡＰ５が、複数の無線ＬＡＮアクセスポイント部５２を有する場合、各々の無線ＬＡＮアクセスポイント部５２毎に異なる無線グループＩＤおよび無線ＬＡＮ用暗号化キーを設定することで、会議時、ＭＦＡＰ５内の無線ＬＡＮアクセスポイント部５２に接続される端末４の数を均等化することができ、無線区間におけるトラフィックの低下を防止できる。この場合、内蔵する無線ＬＡＮアクセスポイント部５２の数分だけ無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、内蔵する無線ＬＡＮアクセスポイント部５２に、登録された会議参加者が均等になるように割り当て（Ｓ２０１）、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（Ｓ２０２）。この参加者宛ての電子メールには、会議の日時、ＭＦＡＰ５が会議で割り当てた無線ＬＡＮアクセスポイント部５２の設定情報である無線グループＩＤ、無線ＬＡＮ用暗号化キー、会議で使用する１人分のアカウントおよび１人分のパスワードが記載されている。

【００３９】各会議参加者は、ＭＦＡＰ５から送られてきた電子メールを会議で使用する端末４に渡し、会議システム（ソフトウェア）を起動させ、ＭＦＡＰ５から送られてきた電子メールを読み込ませる。会議システムは、読み込んだ電子メールから会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを取り出して記憶する。

【００４０】複数の会議を管理するために、図３に示すような会議スケジュール管理を行う。会議参加者は、会議の日時および場所の情報だけを知ることができるが、会議の無線通信の設定情報やアカウントおよびパスワードについては、会議システムが管理するので、会議参加者は知らなくてもよい。また、第三者の目に触れさせないためにも、会議参加者の目に触れさせない方が望ましい。

【００４１】会議を予約した時間になると、ＭＦＡＰ５は、会議で使用する無線ＬＡＮアクセスポイント部５２における無線グループＩＤおよび無線ＬＡＮ用暗号化キーの設定を不揮発性記憶部５３から読み出して変更する（Ｓ２０３）。

【００４２】参加者は、会議システム（ソフトウェア）が搭載されている端末４を持ち込み、端末４を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループＩＤおよび無線ＬＡＮ用暗号化キーを端末４に接続されている無線ＬＡＮカードに設定する。端末４が無線ＬＡＮを内蔵している場合、内蔵無線ＬＡＮに設定する。

【００４３】そして、会議システムは、無線ＬＡＮの接続要求を行い（無線ＬＡＮ認証要求、Ｓ１０３）、接続完了後（無線ＬＡＮ認証確認、Ｓ１０４）、無線ＬＡＮを経由して同じ電子メールに記載されていたアカウントでＭＦＡＰ５内部の会議システムにログインし（ユーザ認証要求、Ｓ１０５）、パスワードで認証する（ユーザ認証確認、Ｓ１０６）。

【００４４】ＭＦＡＰ５は、アカウント名およびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。会議に代理人を出席させる場合、ＭＦＡＰ５から送られてきた電子メールを転送するか、あるいは記録媒体に記録して代理人に渡す。代理人は、会議に持ち込む端末４に搭載されている会議システムを起動させ、ＭＦＡＰ５から送られてきた電子メールを読み込ませる。出席者は変わっても、会議用のアカウントだけで有効な出席者か否かを判断するので、容易に代理人を出席させることが可能となる。

【００４５】また、同一アカウントのログインが発生した場合、前記第１の実施形態と同様、図４に示す処理が行われる。すなわち、同一のアカウントのログインが発生した場合、一方が不正なログインをしているおそれがある。これを検出するために、ＭＦＡＰ５は、会議が始まると、同一のアカウントのログイン処理を行う。

【００４６】まず、ログイン要求があるまで待ち（ステップＳ１）、ログイン要求があると、同一ログインフラグを調べる（ステップＳ２）。同一ログインフラグが立っていない（セットされていない）場合、今回ログイン要求されたアカウントと同じアカウントからのログイン要求が既にあったか否かを調べる（ステップＳ３）。同じアカウントからのログイン要求がなかった場合、正常なログイン処理を行い（ステップＳ４）、ステップＳ１の処理に戻り、次のログイン要求を待つ。

【００４７】一方、ステップＳ３で同一のアカウントからのログイン要求が既にあった場合、同一のアカウントからのログイン要求があったことを示す同一ログインフラグをセットし（ステップＳ５）、既にログインしている会議出席者の有無を調べる（ステップＳ６）。会議出席者がいない場合、ステップＳ１の処理に戻って、次の

ログイン要求を待つ。一方、既に会議出席者がいる場合、正常にログインした出席者に不正なログインがあった旨の警告を送信する（ステップＳ７）。この後、ステップＳ１の処理に戻る。

【００４８】そして、ステップＳ５で同一のログインフラグがセットされると、次にログイン要求があった場合、ステップＳ２における同一ログインフラグのチェックの結果、この会議には不正なログイン処理が行われている旨の警告を表示し（ステップＳ８）、ステップＳ１の処理に戻る。

【００４９】そして、不正なログインがあると、ＭＦＡＰ５は、会議主催者だけにアクセスを許可する。不正なログインの警告を目にした会議主催者は、ＭＦＡＰ５に会議用設定情報の再発行を依頼する。依頼を受けたＭＦＡＰ５は、会議用設定情報を新たに決定し、その設定用ファイルを会議主催者に渡す。渡された設定用ファイルには、新しい無線グループＩＤ、無線ＬＡＮ用暗号化キー、この会議共通のアカウントおよびパスワードが記載されている。主催者は、記録媒体を使用するかあるいは無線ＬＡＮの１対１通信モードを使用し、他の参加者に新しい会議用設定情報を通知する。不正ログインを行った第三者が、この時点で新たな会議用設定情報を知ることは不可能であるので、会議内容を知ることはできない。ＭＦＡＰ５は、念のため、参加者のログイン数を調べ、予約時に登録されているメールアドレスの数とこのログイン数の比較を行う。

【００５０】全ての出席者のログアウト処理が行われると、ＭＦＡＰ５は、会議終了と判断し、会議終了と判断した会議用のアカウントおよびパスワードを破棄する。また、無線ＬＡＮアクセスポイント部５２の設定を次の会議用のものに変更する。ここで、次の会議の予定がない場合、あるいは次の会議まで長時間ある場合、ランダムに生成した無線グループＩＤおよび無線ＬＡＮ用暗号化キーで設定を変更し、悪意の第三者の不正アクセスを防止する。さらには、長時間に亘って使用されない場合、無線ＬＡＮアクセスポイント部５２あるいは無線ＬＡＮアクセスポイント５の電源を落とし、不正なアクセスを防止するようにしてもよい。

【００５１】尚、電子メールそのものに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載する代わりに、電子メールにファイルを添付し、この添付ファイルに会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載してもよく、同様の動作が実現可能である。

【００５２】このように、会議予約時に発行する電子メールに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載し、参加者の端末に搭載されている会議システムに読み込ませるだけで、自動的に会議に参加でき、しかも第三者による会議内容の盗聴といった悪意ある行為を防止することができる。

【００５３】［第３の実施形態］図７は第３の実施形態における電子会議システムの構成を示す図である。前記第１および第２の実施形態と同一の構成要素は同一の符号で示される。図において、３は有線ＬＡＮである。４は会議で使用する端末である。５は多機能アクセスポイントである。６は会議予約サーバである。

【００５４】多機能アクセスポイントの構成は、図６に示す通り、前記第２の実施形態と同様である。そして、大人数での会議を行った場合、トラフィックの分散を図るために、無線ＬＡＮアクセスポイント部５２は複数存在することもある。

【００５５】図８は第３の実施形態における会議の予約から会議開始時までの処理手順を示すフローチャートである。まず、多機能無線ＬＡＮアクセスポイント（ＭＦＡＰ）５は持ち運び自在であり、有線ＬＡＮ３から切り離されている。有線ＬＡＮ３上には、会議用設定情報を作成する会議予約サーバ６が存在している。ここでは、会議予約サーバ６を用いて、会議の予約を行う場合を示す。また、会議システムサーバの機能はＭＦＡＰ５によって実現されている。

【００５６】会議主催者は、会議予約サーバ６で会議の予約を行う（Ｓ１０１）。予約の際、会議の日時および参加者のメールアドレスを登録する（Ｓ１０２）。一方、会議の予約を受け付けると、会議予約サーバ６は、会議に必要な無線ＬＡＮの無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、また、予約された会議だけで有効なアカウントおよびパスワードを参加者分だけ発行する（Ｓ２０１）。そして、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（Ｓ２０２）。

【００５７】参加者宛ての電子メールには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードが記載されている。電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム（ソフトウェア）同士でのみ有効な符号に置き換えておくことが望ましい。

【００５８】会議予約サーバ６は、ＭＦＡＰ５で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、全ての参加者のアカウントおよびこのアカウントに対応するパスワードを記録し、会議主催者に電子メールで送る（Ｓ２０４）。ここで、ＭＦＡＰ５が複数の無線ＬＡＮアクセスポイント部５２を有する場合、各無線ＬＡＮアクセスポイント部５２毎に、異なる無線グループＩＤおよび無線ＬＡＮ用暗号化キーを設定することで、会議時、ＭＦＡＰ５内の無線ＬＡＮアクセスポイント部５２に接続される端末４の数を均等化することができ、無線区間で

のトラフィックの低下を防止できる。この場合、内蔵する無線ＬＡＮアクセスポイント部５２の数分だけ無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、内蔵する無線ＬＡＮアクセスポイント部５２に、登録された会議参加者が均等になるように割り当て（Ｓ２０１）、登録されたメールアドレスを基に、これらの情報を電子メール内に記載して各参加者に電子メールを送信する（Ｓ２０２）。

【００５９】参加者宛ての電子メールには、会議の日時、ＭＦＡＰ５が会議で割り当てた無線ＬＡＮアクセスポイント部５２の設定情報である無線グループＩＤおよび無線ＬＡＮ用暗号化キー、および会議で使用する１人分のアカウントおよび１人分のパスワードが記載されている。

【００６０】各会議参加者は、会議予約サーバ６から送られてきた電子メールを会議で使用する端末４に渡し、会議システムを起動させ、会議予約サーバ６から送られてきた電子メールを読み込ませる。会議システム（ソフトウェア）は、読み込んだ電子メールから会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを取り出して記憶する。また、複数の会議を管理するために、図３に示すような会議スケジュール管理を行う。会議参加者は、会議の日時および場所の情報だけを知ることができるが、会議の無線通信設定情報やアカウントおよびパスワードは、会議システムが管理するので、会議参加者は知らなくてもよい。また、第三者の目に触れないためにも会議参加者の目に触れさせない方が望ましい。

【００６１】会議主催者は、会議予約サーバ６から送られてきたＭＦＡＰ５用の設定データおよび参加者の認証用データをメモリカードのような着脱自在な記憶媒体（着脱式記憶部）に記録し、これを会議開始前にＭＦＡＰ５の着脱式記憶部５４に装着し、会議用設定情報をＭＦＡＰ５に読み込ませる（Ｓ２０５）。ＭＦＡＰ５は、着脱式記憶部５４の記録媒体中に記録されている無線グループＩＤおよび無線ＬＡＮ用暗号化キーを無線ＬＡＮアクセスポイント部５２に設定する。

【００６２】参加者は、会議システムが搭載されている端末４を持ち込み、端末４を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループＩＤおよび無線ＬＡＮ用暗号化キーを、端末４に接続されている無線ＬＡＮカードに設定する。端末４が無線ＬＡＮを内蔵する場合、内蔵無線ＬＡＮに設定する。

【００６３】会議システムは、無線ＬＡＮの接続を要求し（無線ＬＡＮ認証要求、Ｓ１０３）、接続完了後（無線ＬＡＮ認証確認、Ｓ１０４）、無線ＬＡＮを経由して同じ電子メールに記載されていたアカウントでＭＦＡＰ５内部の会議システムにログインし（ユーザ認証要求、Ｓ１０５）、パスワードで認証する（ユーザ認証確認、Ｓ１０６）。

【００６４】ＭＦＡＰ５は、着脱式記憶部５４に装着された記憶媒体に記載されたアカウントおよびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。会議に代理人を出席させる場合、ＭＦＡＰ５から送られてきた電子メールを転送するか、あるいは記録媒体に記録して代理人に渡す。代理人は会議に持ち込む端末４に搭載されている会議システムを起動し、会議予約サーバ６から送られてきた電子メールを読み込ませる。出席者は変わっても、会議用のアカウントだけで有効な出席者か否かを判断するので、容易に代理人を出席させることが可能となる。

【００６５】また、同一アカウントのログインが発生した場合、前記第１の実施形態と同様、図４に示す処理が行われる。すなわち、同一のアカウントのログインが発生した場合、一方が不正なログインをしているおそれがある。これを検出するために、ＭＦＡＰ５は、会議が始まると、アカウントのログイン処理を行う。

【００６６】まず、ログイン要求があるまで待ち（ステップＳ１）、ログイン要求があると、同一ログインフラグを調べる（ステップＳ２）。同一ログインフラグが立っていない（セットされていない）場合、今回ログイン要求されたアカウントと同じアカウントからのログイン要求が既にあったか否かを調べる（ステップＳ３）。同じアカウントからのログイン要求がなかった場合、正常なログイン処理を行い（ステップＳ４）、ステップＳ１の処理に戻り、次のログイン要求を待つ。

【００６７】一方、ステップＳ３で同一のアカウントからのログイン要求が既にあった場合、同一のアカウントからのログイン要求があったことを示す同一ログインフラグをセットし（ステップＳ５）、既にログインしている会議出席者の有無を調べる（ステップＳ６）。会議出席者がいない場合、ステップＳ１の処理に戻って、次のログイン要求を待つ。一方、既に会議出席者がいる場合、正常にログインした出席者に不正なログインがあった旨の警告を送信する（ステップＳ７）。この後、ステップＳ１の処理に戻る。

【００６８】そして、ステップＳ５で同一ログインフラグがセットされると、次にログイン要求があった場合、ステップＳ２における同一ログインフラグのチェックの結果、この会議には不正なログイン処理が行われている旨の警告を表示し（ステップＳ８）、ステップＳ１の処理に戻る。

【００６９】そして、不正なログインがあると、ＭＦＡＰ５は、会議主催者だけにアクセスを許可する。不正なログインの警告を目にした会議主催者は、ＭＦＡＰ５に会議用設定情報の再発行を依頼する。依頼を受けたＭＦＡＰ５は、会議用設定情報を新たに決定し、新たな設定用のファイルを着脱式記憶部５４の記録媒体に書き込

む。この記録媒体には、新しい無線グループＩＤ、無線ＬＡＮ用暗号化キー、この会議共通のアカウントおよびパスワードが記録されている。主催者は、この記録媒体を他の参加者に渡すか、あるいは無線ＬＡＮの１対１通信モードを使用し、他の参加者に新しい会議用設定情報を通知する。不正ログインを行った第三者が、この時点で新たな会議用設定情報を知ることは不可能であるので、会議内容を知ることはできない。ＭＦＡＰ５は、念のため、参加者のログイン数を調べ、予約時に登録されているメールアドレスの数とこのログイン数の比較を行う。

【００７０】全ての出席者のログアウト処理が行われると、ＭＦＡＰ５は、会議終了と判断し、会議終了と判断した会議用のアカウントおよびパスワードを破棄する。さらに、無線ＬＡＮアクセスポイント部５２だけ電源を落とすか、ＭＦＡＰ５の全ての電源を落とし、不正なアクセスを防止する。

【００７１】尚、電子メールそのものに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載する代わりに、電子メールにファイルを添付するようにしてもよい。この添付ファイルには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードが記載されていればよく、同様の動作を実現可能である。

【００７２】このように、第３の実施形態では、会議予約時に発行する電子メールに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載し、参加者が所有する端末に搭載されている会議システムにこれらの会議用設定情報を読み込ませるだけで、自動的に会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる。

【００７３】［第４の実施形態］図９は第４の実施形態における電子会議システムの構成を示す図である。前記第１、第２および第３の実施形態と同一の構成要素については、同一の符号を付すことにする。図において、４は会議で使用する端末である。５は多機能アクセスポイントである。

【００７４】多機能アクセスポイント５の内部構成は、図６に示す通り、前記第２の実施形態と同様である。すなわち、多機能アクセスポイント５は、制御部５１、無線ＬＡＮアクセスポイント部５２、不揮発性記憶部５３、着脱式記憶部５４および有線ＬＡＮインターフェイス５５を有する。この無線ＬＡＮアクセスポイント部５２は、大人数での会議を行った場合、トラフィックの分散を図るために、複数存在する場合もある。

【００７５】図１０は第４の実施形態における会議の予約から会議開始までの処理手順を示すフローチャートである。多機能無線ＬＡＮアクセスポイント（ＭＦＡＰ）５は持ち運び自在であり、随時、有線ＬＡＮ３に接続される。ここでは、会議予約時に有線ＬＡＮ３に接続し、ＭＦＡＰ５で会議を予約する場合を示す。

【００７６】ＭＦＡＰ５は、ＤＨＣＰクライアント機能を有し、起動時に接続されている有線ＬＡＮ３にネットワークアドレスが割り当てられるように、ＭＦＡＰ５に対し、ＤＨＣＰサーバに関する設定を行うとともに、電子メールサーバに関する情報を設定しておく必要がある。

【００７７】会議主催者は、ＭＦＡＰ５を有線ＬＡＮ３に接続した状態で起動する。主催者は、ＭＦＡＰ５にログインして会議の予約を行う（Ｓ１０１）。予約の際、会議の日時および参加者のメールアドレスを登録する（Ｓ１０２）。会議の予約を受け付けると、ＭＦＡＰ５は、会議に必要な無線ＬＡＮの無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、さらに予約された会議だけで有効なアカウントおよびパスワードを参加者分だけ発行する（Ｓ２０１）。

【００７８】登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（Ｓ２０２）。参加者宛ての電子メールには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードが記載されている。尚、電子メールに記載されたこれらの会議用設定情報は、通常のテキストデータであってもよいが、会議システム（ソフトウェア）同士だけで有効な符号に置き換えておくことが望ましい。

【００７９】ＭＦＡＰ５は、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、全ての参加者のアカウント、およびこれらのアカウントに対応するパスワードを、ＭＦＡＰ５内部の不揮発性記憶部５３に記録する。一連の予約受付が終了すると、ＭＦＡＰ５本体の表示部（図示せず）で表示するか、会議主催者に電子メールで予約受付終了を通知する（Ｓ２０６）。

【００８０】ＭＦＡＰ５が、複数の無線ＬＡＮアクセスポイント部５２を有する場合、各々の無線ＬＡＮアクセスポイント部５２毎に異なる無線グループＩＤおよび無線ＬＡＮ用暗号化キーを設定することで、会議時、ＭＦＡＰ５内の無線ＬＡＮアクセスポイント部５２に接続する端末４の数を均等化することができ、無線区間でのトラフィックの低下を防止することができる。この場合、内蔵する無線ＬＡＮアクセスポイント５２の数分だけ無線グループＩＤおよび無線ＬＡＮ用暗号化キーを決定し、内蔵する無線ＬＡＮアクセスポイント部５２に、登録された会議参加者が均等になるように割り当てる（Ｓ２０１）。そして、登録されたメールアドレスを基に、これらの情報を電子メール内に記載し、各参加者に電子メールを送る（Ｓ２０２）。参加者宛ての電子メールには、会議の日時、ＭＦＡＰ５が割り当てた無線ＬＡＮアクセスポイント部５２の設定情報である無線グループＩ

Dおよび無線ＬＡＮ用暗号化キー、および会議で使用する１人分のアカウントおよび１人分のパスワードが記載されている。

【００８１】各会議参加者は、ＭＦＡＰ５から送られてきた電子メールを会議で使用する端末４に渡し、会議システムを起動させ、ＭＦＡＰ５から送られてきた電子メールを読み込ませる。会議システムは、読み込んだ電子メールから会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを取り出して記憶する。また、複数の会議を管理するために、図３に示す会議スケジュール管理を行う。会議参加者は、会議の日時および場所の情報だけを知ることができるが、会議の無線通信の設定情報やアカウントおよびパスワードについては、会議システムが管理するので、会議参加者は知らなくてもよい。また、第三者の目に触れさせないためにも、会議参加者の目に触れさせない方が望ましい。

【００８２】会議主催者は、会議時、予約を行ったＭＦＡＰ５を会議室に持ち込み、起動させる。ＭＦＡＰ５が起動すると、不揮発性記憶部５３から会議用設定情報を読み込み、無線グループＩＤおよび無線ＬＡＮ用暗号化キーを無線ＬＡＮアクセスポイント部５２に設定する（Ｓ２０７）。

【００８３】参加者は、会議システムが搭載されている端末４を持ち込み、端末４を立ち上げ、会議システムを起動する。起動した会議システムは、予め読み込んだ電子メールに記載されていた会議で使用する無線グループＩＤおよび無線ＬＡＮ用暗号化キーを、端末４に接続されている無線ＬＡＮカードに設定する。端末４が無線ＬＡＮを内蔵している場合、内蔵無線ＬＡＮに設定する。

【００８４】会議システムは、無線ＬＡＮの接続を要求し（無線ＬＡＮ認証要求、Ｓ１０３）、接続完了後（無線ＬＡＮ認証確認、Ｓ１０４）、無線ＬＡＮを経由して同じ電子メールに記載されていたアカウントでＭＦＡＰ５内部の会議システムにログインし（ユーザ認証要求、Ｓ１０５）、パスワードで認証する（ユーザ認証確認、Ｓ１０６）。ＭＦＡＰ５は、不揮発性記憶部５３に記憶されたアカウントおよびパスワードを参照し、有効なアカウント名である場合、会議に参加させる。

【００８５】会議に代理人を出席させる場合、ＭＦＡＰ５から送られてきた電子メールを、電子メールで転送するか、あるいは記録媒体に記録して代理人に渡す。代理人は会議に持ち込む端末４に搭載されている会議システムを起動させ、ＭＦＡＰ５から送られてきた電子メールを会議システムに読み込ませる。出席者は変わっても、会議用のアカウントだけで有効な出席者であるか否かを判断するので、容易に代理人を出席させることが可能である。尚、同一のアカウントのログインが発生した場合の処理は、前記第３の実施形態と同様である。

【００８６】そして、全ての出席者のログアウト処理が行われると、ＭＦＡＰ５は、会議終了と判断し、会議終了と判断した会議用のアカウントおよびパスワードを破棄する。さらに、無線ＬＡＮアクセスポイント部５２だけ電源を落とすか、あるいはＭＦＡＰ５の全ての電源を落として、不正なアクセスを防止する。

【００８７】電子メールそのものに、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載する代わりに、電子メールにファイルを添付してもよい、この添付ファイルには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードが記載されていればよく、同様の動作を実現できる。

【００８８】このように、会議予約時に発行する電子メールには、会議の日時、会議で使用する無線グループＩＤ、無線ＬＡＮ用暗号化キー、１人分のアカウントおよび１人分のパスワードを記載し、参加者の端末に搭載されている会議システムに読み込ませるだけで、自動的に会議に参加でき、しかも、第三者による会議内容の盗聴するといった悪意ある行為を防止できる。

【００８９】以上が本発明の実施の形態の説明であるが、本発明は、これら実施の形態の構成に限られるものではなく、特許請求の範囲で示した機能、または実施の形態の構成が持つ機能が達成できる構成であればどのようなものであっても適用可能である。

【００９０】また、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードをシステムあるいは装置に供給することによって達成される場合、プログラムコード自体が本発明の新規な機能を実現することになり、そのプログラム自体およびそのプログラムを記憶した記憶媒体は本発明を構成することになる。このプログラムコードが格納される記憶媒体としては、ＲＯＭ、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ、不揮発性のメモリカードなどを用いることができる。

【００９１】

【発明の効果】本発明によれば、参加者が特別な作業を行うことなく会議に参加でき、しかも、第三者による会議内容の盗聴といった悪意ある行為を防止できる。

【図面の簡単な説明】

【図１】第１の実施形態における電子会議システムの構成を示す図である。

【図２】会議の予約から会議開始時までの動作処理手順を示すフローチャートである。

【図３】会議スケジュール管理を示す図である。

【図４】アカウントのログイン処理手順を示すフローチャートである。

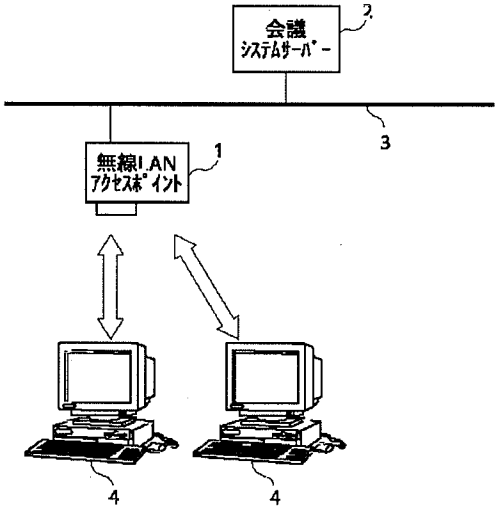
【図５】第２の実施形態における電子会議システムの構成を示す図である。

【図６】多機能アクセスポイントの内部構成を示すブロ

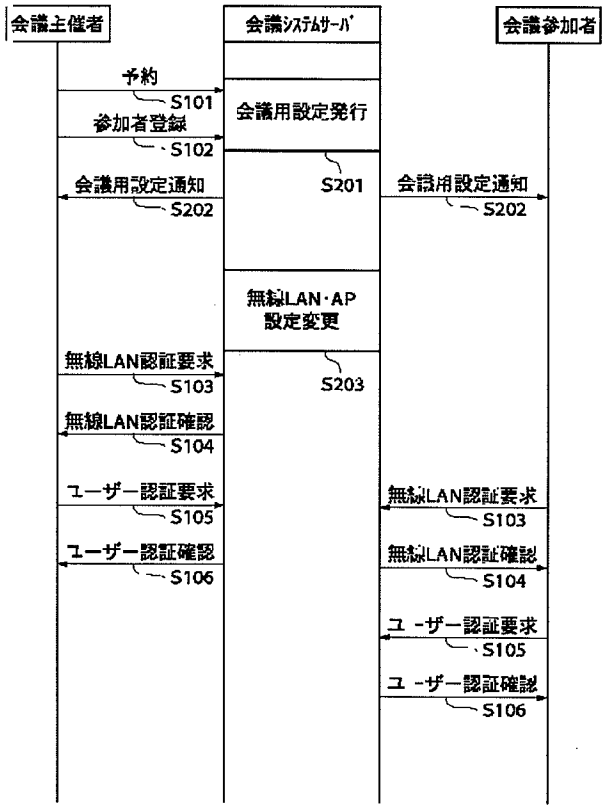
ック図である。
【図７】第３の実施形態における電子会議システムの構成を示す図である。
【図８】第３の実施形態における会議の予約から会議開始時までの処理手順を示すフローチャートである。
【図９】第４の実施形態における電子会議システムの構成を示す図である。
【図１０】第４の実施形態における会議の予約から会議開始までの処理手順を示すフローチャートである。
【符号の説明】

１　無線ＬＡＮアクセスポイント
２　会議システムサーバ
３　有線ＬＡＮ
４　端末
５　多機能アクセスポイント
６　会議予約サーバ
５１　制御部
５２　無線ＬＡＮアクセスポイント部
５３　不揮発性記憶部
５４　着脱式記憶部

【図１】



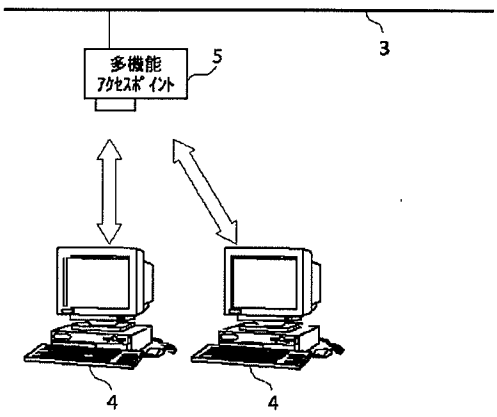
【図２】



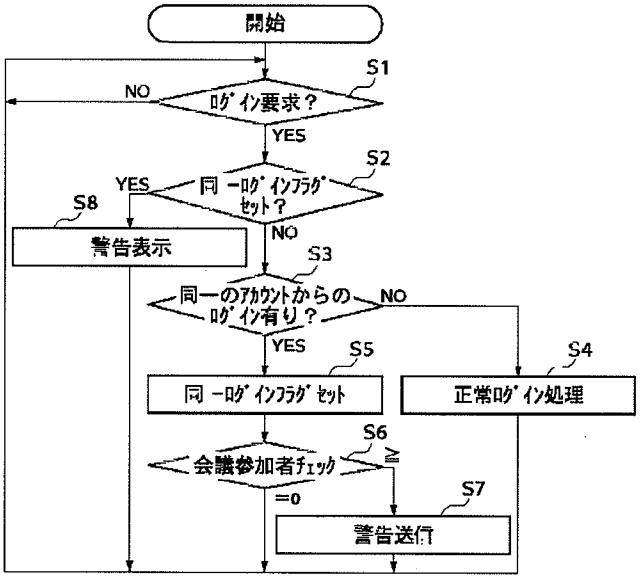
【図３】

ユーザーに見える情報	ユーザーに見えない情報
打ち合わせ ○月△日××時	ESSID：□○△× WEP：□□○× USER：○□△× PASS：××××
打ち合わせ ○月□日××時	ESSID：○○○△ WEP：△△□○ USER：○○△□ PASS：×○×○

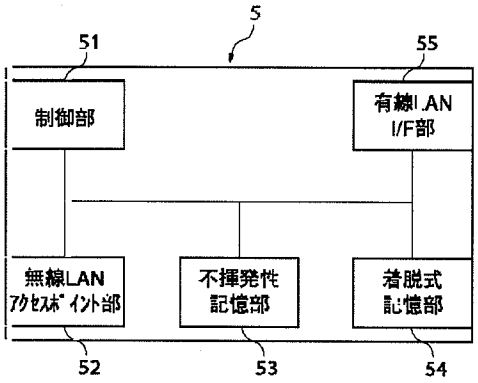
【図５】



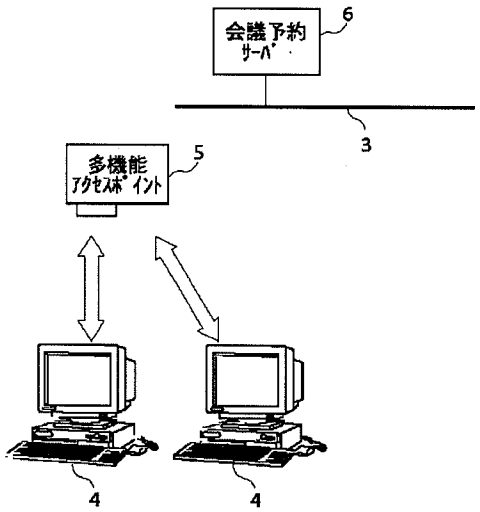
【図4】


開始
S1
NO
ログイン要求？
YES
S2
YES
同一ログインフラグセット？
S8
警告表示
NO
S3
同一のアカウントからのログイン有り？
NO
YES
S5
S4
同一ログインフラグセット
正常ログイン処理
S6
会議参加者チェック
≧
=0
S7
警告送信

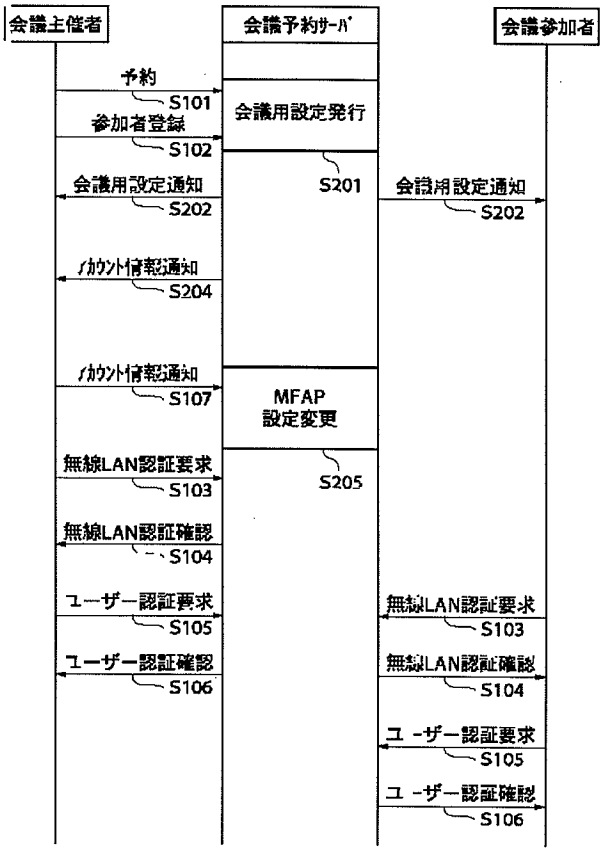
【図6】


5
51
55
制御部
有線LAN I/F部
無線LAN アクセスポイント部
不揮発性記憶部
着脱式記憶部
52
53
54

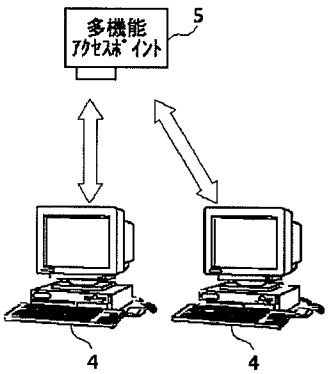
【図7】


会議予約サーバ
6
3
多機能アクセスポイント
5
4
4

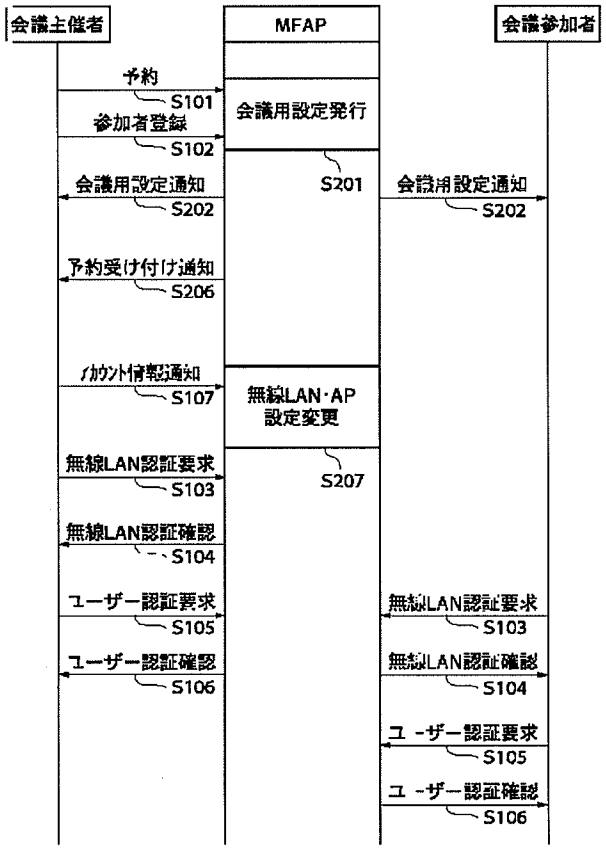
【図8】


会議主催者
会議予約サーバ
会議参加者
予約
S101
会議用設定発行
参加者登録
S102
S201
会議用設定通知
S202
会議用設定通知
S202
アカウント情報通知
S204
アカウント情報通知
S107
MFAP設定変更
S205
無線LAN認証要求
S103
無線LAN認証確認
S104
ユーザー認証要求
S105
ユーザー認証確認
S106
無線LAN認証要求
S103
無線LAN認証確認
S104
ユーザー認証要求
S105
ユーザー認証確認
S106

【図9】


多機能アクセスポイント
5
4
4

【図１０】


会議主催者
MFAP
会議参加者
予約
S101
参加者登録
S102
会議用設定発行
S201
会議用設定通知
S202
会議用設定通知
S202
予約受け付け通知
S206
アカウント情報通知
S107
無線LAN・AP
設定変更
S207
無線LAN認証要求
S103
無線LAN認証確認
S104
ユーザー認証要求
S105
ユーザー認証確認
S106
無線LAN認証要求
S103
無線LAN認証確認
S104
ユーザー認証要求
S105
ユーザー認証確認
S106